Résolution des défaillances DMARC en corrigeant l'alignement SPF et DKIM

Table des matières

Problème

Les e-mails provenant de domaines spécifiques sont bloqués par la passerelle de messagerie sécurisée Cisco (CES/ESA) en raison d'échecs de vérification DMARC. L'analyse du suivi des messages indique que ces messages sont conservés dans la file d'attente de travail et placés en quarantaine ou rejetés, ce qui les empêche d'atteindre les destinataires prévus.

Environnement

- Appareils Cisco Secure Email Gateway (CES/ESA)
- Les politiques SPF, DKIM et DMARC sont configurées et appliquées

Résolution

Tableau récapitulatif d'alignement SPF/DKIM (exemples)

Mécanisme	État d'alignement	Domaine d'enveloppe/signature	Du domaine d'en-tête	Logique
FPS	Alignement	sender@example.com	sender@example.com	Correspondance directe

FPS	Alignement	sender@child.example.com	sender@example.com	Correspondance du domaine parent
FPS	Non aligné	sender@test.com	sender@example.com	Non-concordance de domaine
DKIM	Alignement	example.com	sender@example.com	Correspondance directe
DKIM	Alignement	example.com	sender@child.example.com	Correspondance de mode relaxé
DKIM	Non aligné	example.com	sender@test.com	Non-concordance de domaine

Coordonner avec l'expéditeur (recommandé)

- Collaborer avec les administrateurs du domaine expéditeur pour corriger les défaillances DMARC en garantissant un alignement SPF et DKIM approprié au niveau de l'en-tête.
- L'expéditeur doit :
    - Assurez-vous que le domaine utilisé dans l'identité MAIL FROM ou HELO/EHLO validée par SPF correspond au domaine dans l'en-tête From de l'e-mail.
    - Implémentez la signature DKIM où le domaine spécifié dans la balise d= de la signature DKIM s'aligne sur le domaine d'en-tête From.
    - Vérifiez que la stratégie DMARC est correctement configurée pour appliquer le mode d'alignement (strict ou relâché) et les options de rapport souhaités.
- Cette approche s'attaque à la cause première des défaillances DMARC en se concentrant sur l'alignement des domaines authentifiés avec le domaine d'en-tête D visible, qui est essentiel pour la remise à long terme des e-mails.

Créer une exception DMARC (alternative)

- Si la correction par l'expéditeur n'est pas possible, créez une exception sur le périphérique ESA pour l'adresse de l'expéditeur spécifique afin de contourner les vérifications DMARC.
- Il s'agit d'une solution de contournement temporaire qui doit être accompagnée d'une surveillance.

Surveiller et valider

- Une fois les modifications implémentées, surveillez la remise des e-mails d'alerte aux destinataires prévus.
- Vérifiez les journaux de suivi des messages pour confirmer que les défaillances DMARC ont été résolues.
- Poursuivez l'analyse des données de suivi des messages mises à jour si les problèmes de remise persistent.

Motif

La principale cause de quarantaine ou de rejet des e-mails est l'échec de la vérification DMARC en raison de problèmes d'alignement SPF et DKIM. Ces défaillances indiquent que, bien que les enregistrements SPF et DKIM puissent être correctement publiés, les domaines authentifiés lors de l'échange d'e-mails ne correspondent pas au domaine d'en-tête De, ce qui entraîne la mise en quarantaine des e-mails.

Présentation de l'alignement DMARC, SPF et DKIM :

- SPF authentifie le domaine dans les commandes SMTP MAIL FROM ou HELO/EHLO et exige que ce domaine soit aligné avec le domaine dans l'en-tête From pour la conformité DMARC.
- DKIM utilise des signatures cryptographiques avec un domaine de signature spécifié dans la balise d=, qui doit être aligné avec le domaine d'en-tête From.
- DMARC s'appuie sur SPF et DKIM en exigeant qu'au moins un de ces domaines authentifiés s'aligne sur le domaine d'en-tête From, soit exactement (mode strict), soit en tant que sous-domaine (mode relâché).

L'échec de cet alignement de domaine entraîne des échecs DMARC et un rejet ou une

quarantaine des e-mails ultérieurs, même si les enregistrements SPF et DKIM eux-mêmes sont correctement publiés et valides.

Ce focus d'alignement garantit que l'identité authentifiée correspond à l'identité de l'expéditeur visible, empêchant l'usurpation et améliorant la fiabilité des e-mails.

Autres informations utiles

- Informations d'alignement SPF
- Informations d'alignement DKIM
- Meilleures pratiques pour l'authentification des e-mails - Méthodes optimales de déploiement de SPF, DKIM et DMARC - Cisco
- Configuration du filtre entrant en fonction de la vérification DKIM dans ESA - Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.